NOKIA

© Nokia
Networks Oy

GPRS Architecture: Interfaces and Protocols

Training Document

GPRS System Course

© Nokia
Networks Oy

The information in this document is subject to change without notice and describes only the product defined in the introduction of this documentation. This document is intended for the use of Nokia Networks' customers only for the purposes of the agreement under which the document is submitted, and no part of it may be reproduced or transmitted in any form or means without the prior written permission of Nokia Networks. The document has been prepared to be used by professional and properly trained personnel, and the customer assumes full responsibility when using it. Nokia Networks welcomes customer comments as part of the process of continuous development and improvement of the documentation.

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products cannot be considered binding but shall be defined in the agreement made between Nokia Networks and the customer. However, Nokia Networks has made all reasonable efforts to ensure that the instructions contained in the document are adequate and free of material errors and omissions. Nokia Networks will, if necessary, explain issues which may not be covered by the document.

Nokia Networks' liability for any errors in the document is limited to the documentary correction of errors. Nokia Networks WILL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT OR FOR ANY DAMAGES, INCIDENTAL OR CONSEQUENTIAL (INCLUDING MONETARY LOSSES), that might arise from the use of this document or the information in it.

This document and the product it describes are considered protected by copyright according to the applicable laws.

NOKIA logo is a registered trademark of Nokia Corporation.

Other product names mentioned in this document may be trademarks of their respective companies, and they are mentioned for identification purposes only.

Copyright © Nokia Networks Oy 2004. All rights reserved.

Contents

© Nokia
Networks Oy

1 Introduction

GPRS provides mobile users access to value-added WAP services and different external packet switched networks. These networks can be, for example, the Internet or corporate intranets. The GSM-BSS provides the radio interface, and the GPRS core network handles mobility and access to external packet networks and services. This is shown in Figure 1.

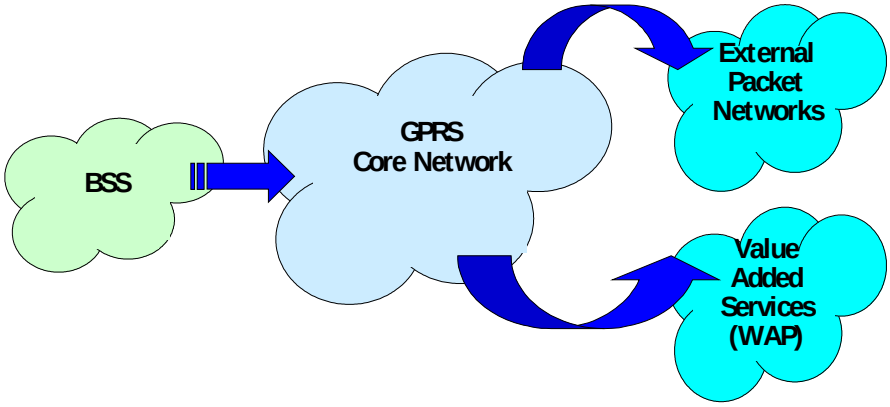

Figure 1. GPRS access to packet switched networks

The GPRS network acts in parallel with the GSM network, providing packet switched connections to the external networks. The requirements of a GPRS network are the following:

- The GPRS network must use as much of the existing GSM infrastructure with the smallest number of modifications to it.
- Since a GPRS user may be on more than one data session, GPRS should be able to support one or more packet-switched connections.
- To support the budgets of various GPRS users, it must be able to support different Quality of Service (QoS) subscriptions of the user.
- The GPRS network architecture has to be compatible with future 3rd and 4th generation mobile communication systems.
- It should be able to support both point-to-point and point-to-multipoint data connections.
- It should provide secure access to external networks.

A GPRS network must provide all of the functionality of a GSM network for packet switched networks and more. The GPRS is expected to perform the functions of a traditional mobile communication network and a traditional packet switched computer network. These functions are itemised below:

- Capability to separate circuit switched and packet switched traffic from mobile station (MS)
- Radio resource management, that is, allocation of radio resources to GPRS subscribers across the air interface
- Interfaces to Internet, intranets, Public Data Networks (PDN), and other Public Land Mobile Networks (PLMN)
- Authenticate subscriber requests for packet switched resources
- Encrypt data transmitted on the air interface for security purposes
- Data compression for data transmitted over the air interface
- Interact with databases (HLR/VLR) containing subscriber information such as IMSI, security data, and subscription information
- Mobility management as in GSM
- Location management as in GSM
- Handover as a GPRS subscriber moves within a coverage area
- Power control to minimise the transmitted power by the user
- Network management that facilitates GPRS network management
- Generation and collection of network performance statistics
- Generation and collection of charging or billing information
- Signalling links between the GPRS network elements
- Routing of packets to appropriate destination
- Protocol conversion between networks that may use different protocols
- Buffering of data at GPRS nodes
- Allocation of static or dynamic address for packets originating from MS
- Protection of the GPRS network from security threats
- Capability to monitor target subscriber by law enforcement agencies
- Translation between logical names and IP addresses using Domain Name System (DNS)
- Facilitation of roaming subscribers so that they can connect to home networks

© Nokia
Networks Oy

- Delivery of SMS messages through the GPRS network
- Redundancy mechanisms if one or more network elements were to fail
- Translation between private and public addresses using NAT and NAPT
- Detection of faulty or stolen GPRS handsets

2 Network elements

Figure 2 shows the architecture of a GPRS network. The GPRS system brings some new network elements to an existing GSM network. These elements are:

- Packet Control Unit (PCU)
- Serving GPRS Support Node (SGSN): the MSC of the GPRS network
- Gateway GPRS Support Node (GGSN): gateway to external networks
- Border Gateway (BG): a gateway to other PLMN
- Intra-PLMN backbone: an IP based network inter-connecting all the GPRS elements
- Charging Gateway (CG)
- Legal Interception Gateway (LIG)
- Domain Name System (DNS)
- Firewalls: used wherever a connection to an external network is required.

Not all of the network elements are compulsory for every GPRS network.

© Nokia
Networks Oy

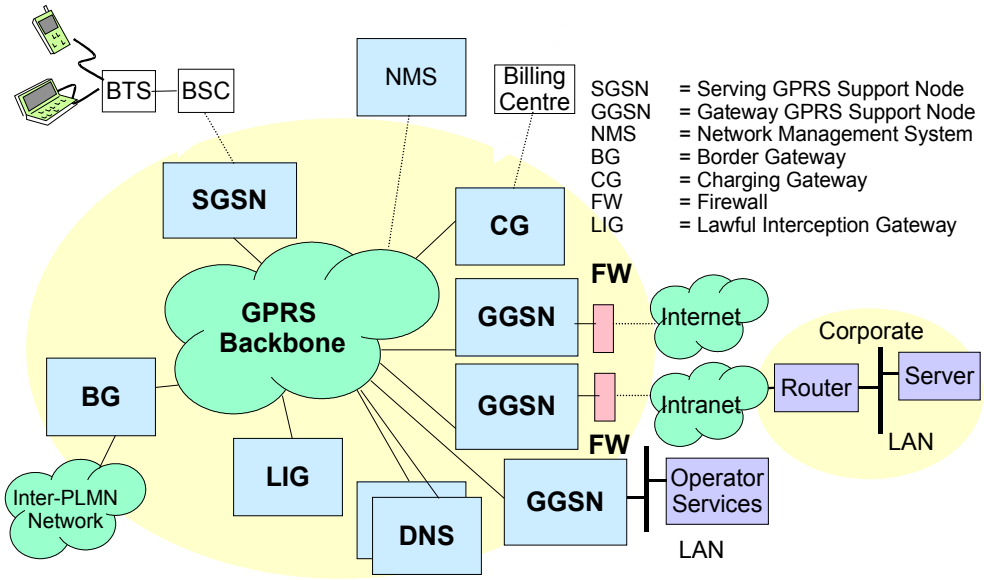

Figure 2. GPRS architecture

2.1 Packet Control Unit (PCU)

The PCU separates the circuit switched and packet switched traffic from the user and sends them to the GSM and GPRS networks respectively. It also performs most of the radio resource management functions of the GPRS network. The PCU can be either located in the BTS, BSC, or some other point between the MS and the MSC. There will be at least one PCU that serves a cell in which GPRS services will be available. Frame Relay technology is being used at present to interconnect the PCU to the GPRS core.

2.2 Serving GPRS Support Node (SGSN)

The SGSN is the most important element of the GPRS network. The SGSN of the GPRS network is equivalent to the MSC of the GSM network. There must at least one SGSN in a GPRS network. There is a coverage area associated with a SGSN. As the network expands and the number of subscribers increases, there may be more than one SGSN in a network. The SGSN has the following functions:

- Protocol conversion (for example IP to FR)
- Ciphering of GPRS data between the MS and SGSN
- Data compression is used to minimise the size of transmitted data units
- Authentication of GPRS users
- Mobility management as the subscriber moves from one area to another, and possibly one SGSN to another
- Routing of data to the relevant GGSN when a connection to an external network is required
- Interaction with the NSS (that is, MSC/VLR, HLR, EIR) via the SS7 network in order to retrieve subscription information
- Collection of charging data pertaining to the use of GPRS users
- Traffic statistics collections for network management purposes.

2.3 Gateway GPRS Support Node (GGSN)

The GGSN is the gateway to external networks. Every connection to a fixed external data network has to go through a GGSN. The GGSN acts as the anchor point in a GPRS data connection even when the subscriber moves to another SGSN during roaming. The GGSN may accept connection request from SGSN that is in another PLMN. Hence, the concept of coverage area does not apply to GGSN. There are usually two or more GGSNs in a network for redundancy purposes, and they back up each other up in case of failure. The functions of a GGSN are given below:

- Routing mobile-destined packets coming from external networks to the relevant SGSN
- Routing packets originating from a mobile to the correct external network
- Interfaces to external IP networks and deals with security issues
- Collects charging data and traffic statistics
- Allocates dynamic or static IP addresses to mobiles either by itself or with the help of a DHCP or a RADIUS server
- Involved in the establishment of tunnels with the SGSN and with other external networks and VPN.

© Nokia
Networks Oy

From the external network's point of view, the GGSN is simply a router to an IP sub-network. This is shown below. When the GGSN receives data addressed to a specific user in the mobile network, it first checks if the address is active. If it is, the GGSN forwards the data to the SGSN serving the mobile. If the address is inactive, the data is discarded. The GGSN also routes mobile originated packets to the correct external network.

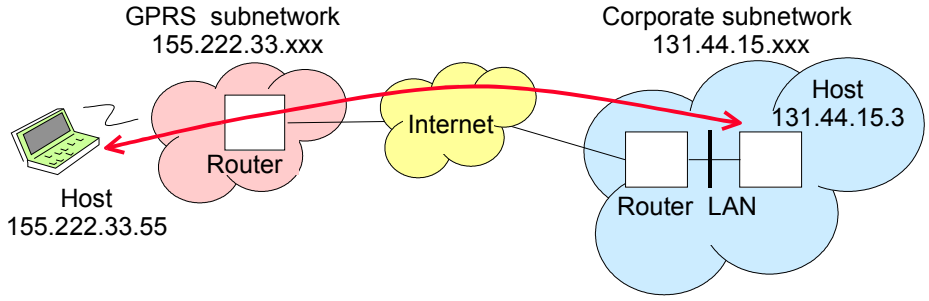

Figure 3. GPRS network as seen by another data network

2.4 Domain Name Servers

These devices convert IP names into IP addresses, for example, server.nokia.com to 133.44.15.5. There is a primary DNS server and a secondary DNS server. Details of DNS were described in *Introduction to TCP/IP* module and in the IPGPRS course Module 10.

2.5 Firewalls

A firewall protects an IP network against external attack (for example, hackers from the mobile users or from the Internet). In the case of GPRS, the firewall might be configured to reject all packets that are not part of a GPRS subscriber-initiated connection. The firewall can also include NAT (Network Address Translation), see the *Introduction to TCP/IP* module.

2.6 Border Gateway

The Border Gateway (BG) is a router that can provide a direct GPRS tunnel between different operators' GPRS networks. This is referred to as an inter-PLMN data network. It is more secure to transfer data between two operators' PLMN networks through a direct connection rather than via the public Internet. The Border Gateway will commence operation once the GPRS roaming agreements between various operators have been signed. It will essentially allow a roaming subscriber to connect to company intranet through the Home GGSN via the visiting PLMN network.

2.7 Charging Gateway

GPRS users have to be charged for the use of the network. In a GSM network, charging is based on the destination, duration, and time of call. However, GPRS offers connectionless service to users, so it not possible to charge subscribers on the connection duration. Charging has to be based on the volume, destination, QoS, and other parameters of a connectionless data transfer. These GPRS charging data are generated by all the SGSNs and GGSNs in the network. This data is referred to as Charging Data Records or CDRs. One data session may generate a number of CDRs, so these need to collected and processed. The Charging Gateway (CG) collects all of these records, sorts them, processes it, and passes it on to the Billing System. Here the GPRS subscriber is billed for the data transaction. All CDRs contain unique subscriber and connection identifiers to distinguish it. A protocol called GTP' (pronounced GTP prime) is used for the transfer of data records between GSNs and the Charging Gateway.

© Nokia
Networks Oy

3 GPRS interfaces

The GPRS system introduces new interfaces to the GSM network. Figure 4 illustrates the logical architecture with the interfaces and reference points of the combined GSM/GPRS network.

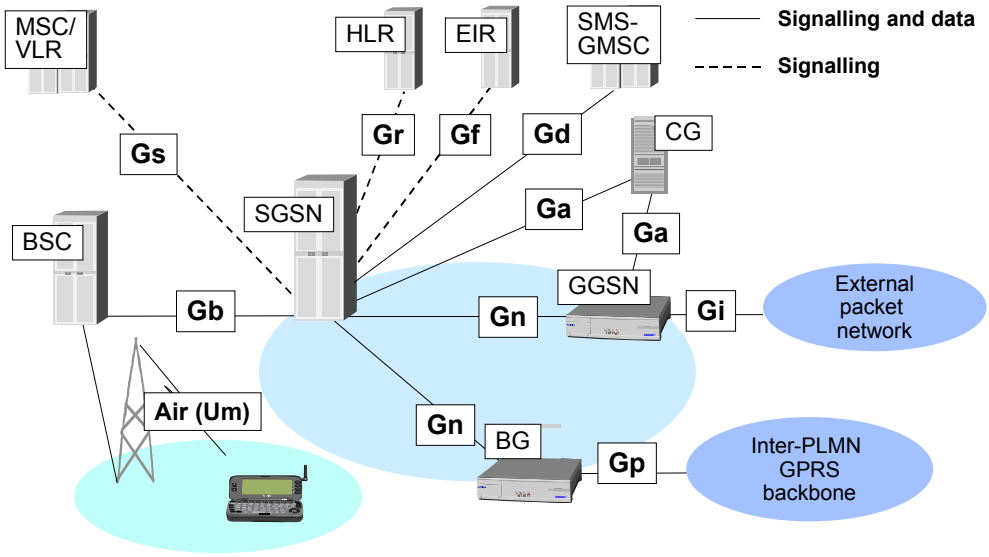

Figure 4. GPRS interfaces

Connections from the GPRS system to the NSS part of the GSM network are implemented through the SS7 network. The GPRS element interfacing with the NSS is SGSN. The important interfaces to the NSS are the SGSN-HLR (Gr), SGSN-EIR (Gf), and SGSN-MSC/VLR (Gs). The other interfaces are implemented through the intra-PLMN backbone network (Gn), the inter-PLMN backbone network (Gp), or the external networks (Gi).

The interfaces used by the GPRS system are described below:

- **Um** between an MS and the GPRS fixed network part. The Um is the access interface the MS uses to access the GPRS network. The radio interface to the BTS is the same interface used by the existing GSM network with some GPRS specific changes.
- **Gb** between a SGSN and a BSS. The Gb interface carries the GPRS traffic and signalling between the GSM radio network (BSS) and the

GPRS network. Frame Relay based network services is used for this interface.

- **Gn** between two GSNs within the same PLMN. The Gn provides a data and signalling interface in the Intra-PLMN backbone. The GPRS Tunnelling Protocol (GTP) is used in the Gn (and in the Gp) interface over the IP based backbone network.
- **Gp** between two GSNs in various PLMNs. The Gp interface provides the same functionality as the Gn interface, but it also provides, together with the BG and the Firewall, all the functions needed for inter-PLMN networking, that is, security, routing, etc.
- **Gr** between an SGSN and the HLR. The Gr gives the SGSN access to subscriber information in the HLR. The HLR can be located in a different PLMN than the SGSN (MAP).
- **Ga** between the GSNs and the CG inside the same PLMN. The Ga provides a data and signalling interface. This interface is used for sending the charging data records generated by GSNs to the CG. The protocol used is GTP', an enhanced version of GTP.
- **Gs** between a SGSN and a MSC. The SGSN can send location data to the MSC or receive paging requests from the MSC via this *optional* interface. The Gs interface will greatly improve the effectiveness of the radio and network resources in the combined GSM/GPRS network. This interface uses BSSAP+ protocol.
- **Gd** between the SMS-GMSC and an SGSN, and between SMS-IWMSC and an SGSN. The Gd interface is available for more efficient use of the SMS services (MAP).
- **Gf** between an SGSN and the EIR. The Gf gives the SGSN access to GPRS user equipment information. The EIR maintains three different lists of mobile equipment: *black list* for stolen mobiles, *grey list* for mobiles under observation and *white list* for other mobiles (MAP).
- **Gc** between the GGSN and the HLR. The GGSN may request the location of an MS via this *optional* interface. The interface can be used if the GGSN needs to forward packets to an MS that is not active.

There are two different **reference points** in the GPRS network. The Gi is GPRS specific, but the R is common with the circuit switched GSM network:

- **Gi** between a GGSN and an external network. The GPRS network is connected to an external data networks via this interface. The GPRS

system will support a variety of data networks. Because of that, the Gi is not a standard interface, but merely a reference point.

- **R** between terminal equipment and mobile termination. This reference point connects terminal equipment to mobile termination, thus allowing, for example, a laptop-PC to transmit data over the GSM-phone. The physical R interface follows, for example, the ITU-T V.24/V.28 or the PCMCIA PC-Card standards.

4 Transfer of packets between GSNs

User data packets are sent over the GPRS backbone in 'containers'. When a packet coming from an external packet network arrives at the GGSN, it is inserted in a container and sent to the SGSN. The stream of containers inside the GPRS backbone network is totally transparent to the user: To the user, it seems like he/she is connected directly via a router (the GGSN) to external networks. In data communications, this type of virtual stream of containers is called a tunnel. We say that the GSNs are performing tunnelling of user packets, see Figure 5.

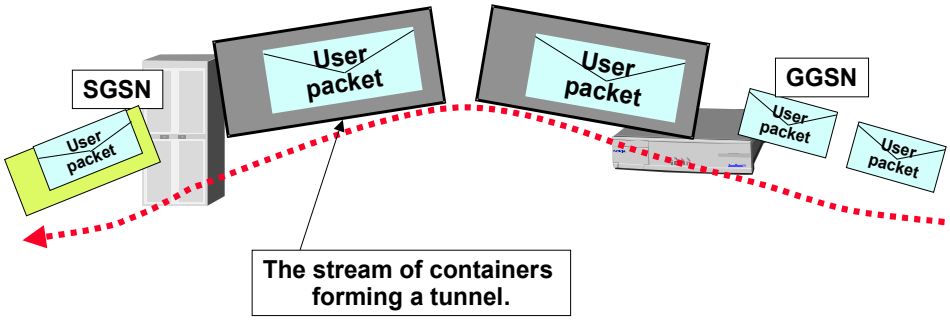

Figure 5. User packets over the GPRS backbone in ‘containers’

The protocol that performs the tunnelling in GPRS is called GPRS Tunnelling Protocol (GTP). We can say that we transport GTP packets between the SGSN and the GGSN.

Over the GPRS backbone, IP packets are used to carry the GTP packets. The GTP packets then contain the actual user packets. This is shown in Figure 6. The user packet, for example, a TCP/IP packet that carries some part of an e-mail, is carried inside a GTP packet. The GTP packet is carried over the GPRS backbone using IP and TCP or UDP (in the example, UDP).

The GTP packet headers, including the tunnel ID (TID), will tell the receiving GSN who the user is. The tunnel ID includes the user IMSI (and another user specific number). The TID is a label that tells the SGSN and the GGSN, whose packets are inside the container.

© Nokia Networks Oy

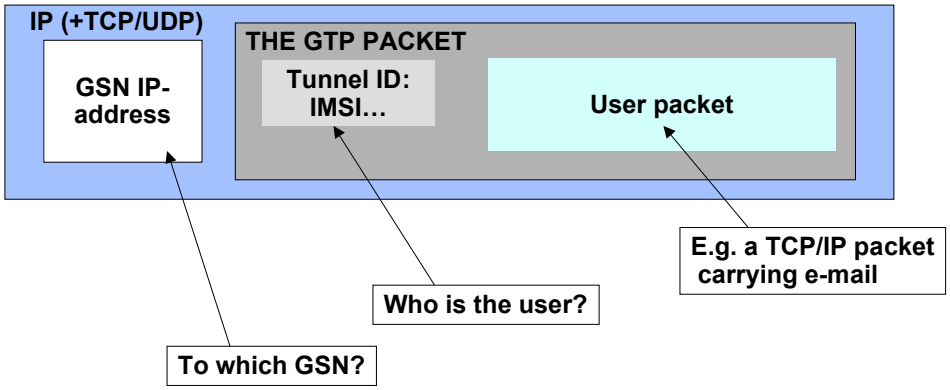

Figure 6. GTP container

From the point of view of the user and the external network, the GTP packets that contain the user packets could be transferred between the GSNs using any technology, for example, ATM, X.25, or Frame Relay. The chosen technology for the GPRS backbone is IP.

All the network elements (the GSNs, the charging gateway, etc.) connected to the GPRS backbone must have an IP address. IP addresses used in the backbone are invisible to the MS and to the external networks. They are what we call **private IP addresses**. That is, the user packets are carried in the GPRS core between the SGSN and the GGSN using the private IP addresses of the GPRS backbone.

This concept of tunnelling and hiding backbone addresses ('private') to the user level is illustrated in the following figures. Figure 7 shows a close-up of the user and backbone IP address levels. Figure 8 shows the GTP tunnel related to the user payload, and the relationship between the protocol stacks in the Gi and Gn interfaces.

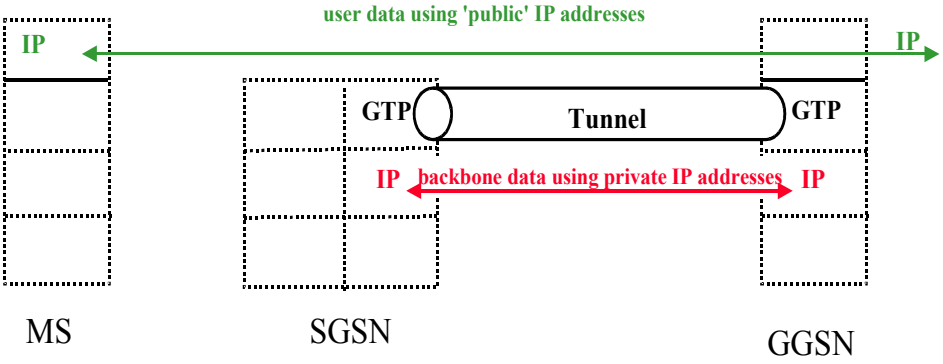

Figure 7. Transfer of packets between the GGSN and the MS

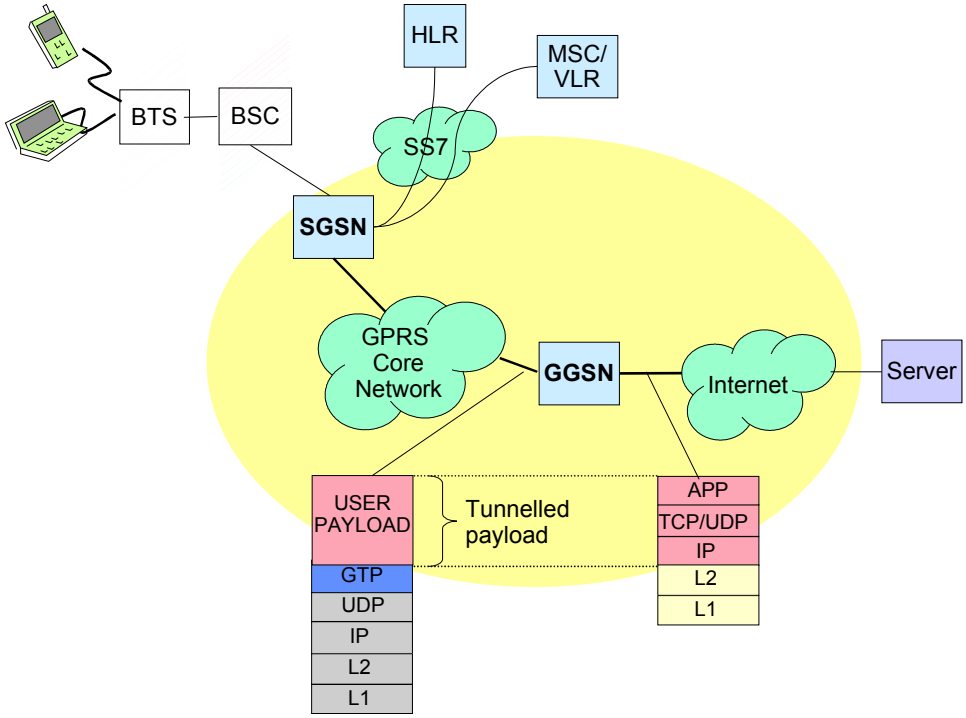

Figure 8. GTP tunnelling and user payload

Note

For additional information on the GPRS transmission protocols, see the Appendix – GPRS transmission plane protocols.

5 Roaming

Here we will look at how GPRS functions when a subscriber is roaming in another network. Before any roaming can take place, roaming agreements need to be signed between various operators. Let us start with an example:

The diplomat boards a plane in Helsinki and departs for Singapore. After a relaxing 11-hour flight she arrives the next morning in Singapore. At the airport, she immediately switches on her GPRS MS.

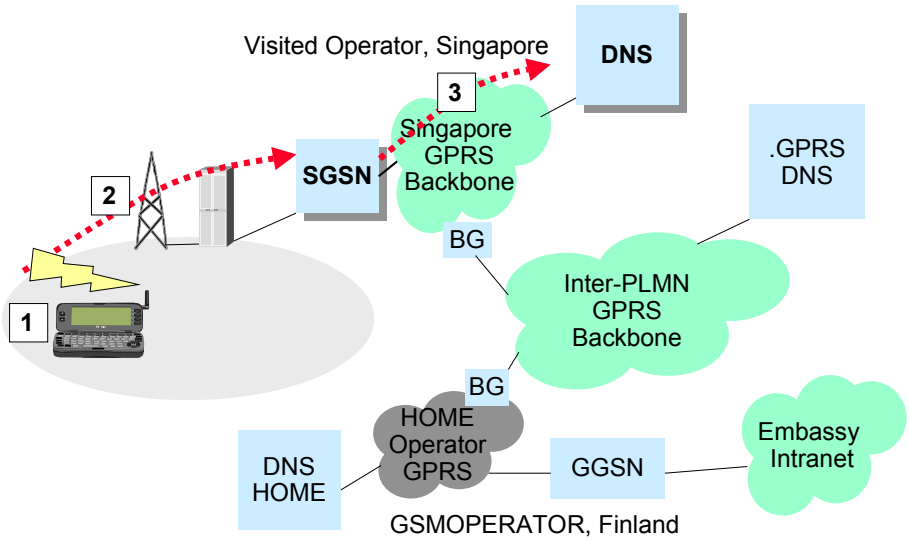

Figure 9. Roaming case steps 1, 2 and 3

1. *The diplomat chooses to use her home network access point, because she wants to securely access her e-mail.*
2. The MS sends the PDP context activation request to the SGSN. An important piece of information is the access point name (APN), which in this case is **embassy.fi.** This is shown in Figure 9. The Singapore operator's SGSN checks with the Gbase if an APN like the one MS requested is permitted in the user's subscription. In this case everything is OK.

3. Now the Singapore SGSN needs to send the context activation creation request to the GSMOPERAOTOR.FI GGSN. The GGSN is somewhere in Finland and the Singapore SGSN does not know the GGSN IP address. So it sends a query to the local DNS in the Singapore operator's network asking the question 'What is the IP address of embassy.fi.'?

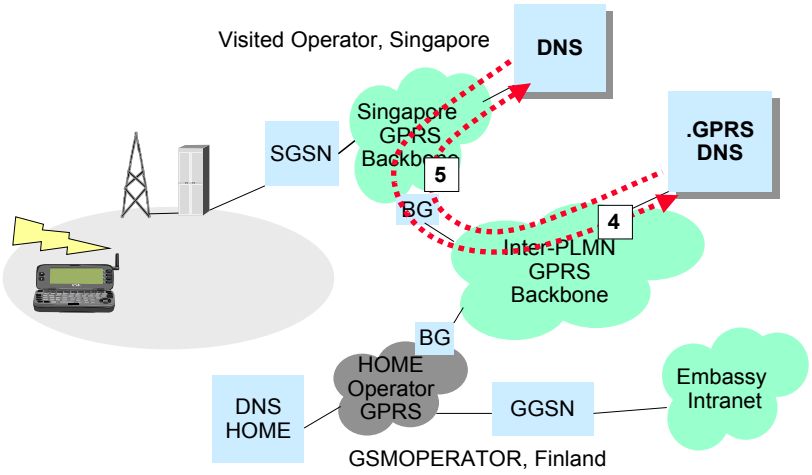

Figure 10. Roaming case step 4 and 5

The next steps are shown in Figure 10 and are described below:

4. The Singapore DNS does not know the **embassy.fi.** IP address, so it forwards the query from the SGSN to the higher-level DNS.

5. The GPRS level does not store IP addresses of APNs (or GGSNs), but instead it stores IP addresses of the operator level DNS servers. The higher-level DNS replies with a list of home operator DNS servers.

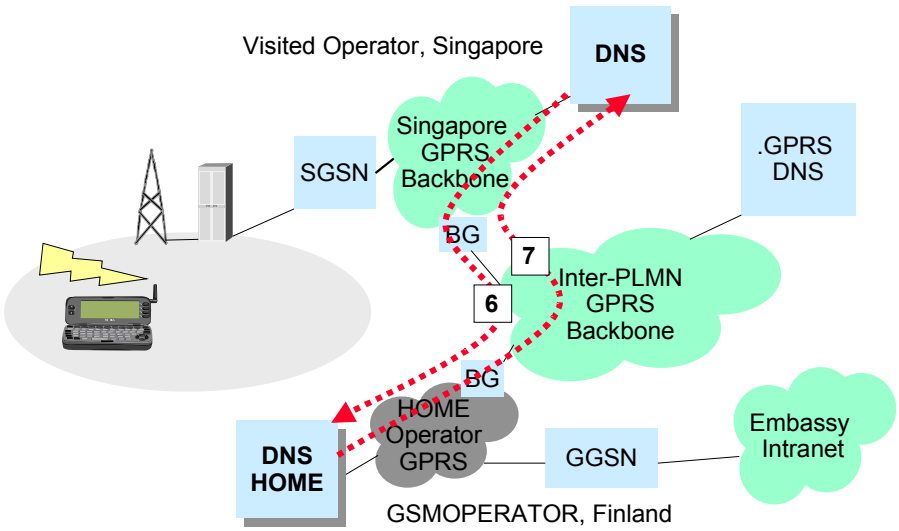

Figure 11. Roaming case steps 6 and 7

6. The Singapore DNS picks one of the DNS servers from the list it received from the higher-level DNS and forwards the original query to this DNS.

7. The GSMOPERATOR DNS replies with the IP address of the GGSN having the access point name **embassy.fi.** as shown in Figure 11.

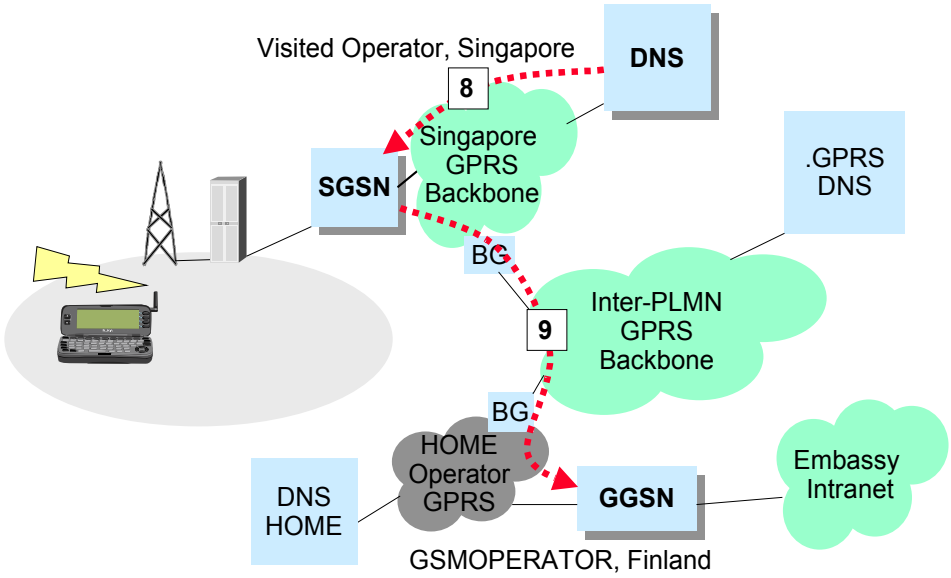

Figure 12. Roaming case steps 8 and 9

8. The Singapore DNS gives the GGSN IP address to the Singapore SGSN.
9. The SGSN sends the GSMOPERATOR GGSN a request to create the context along with the APN. This is shown in Figure 12.

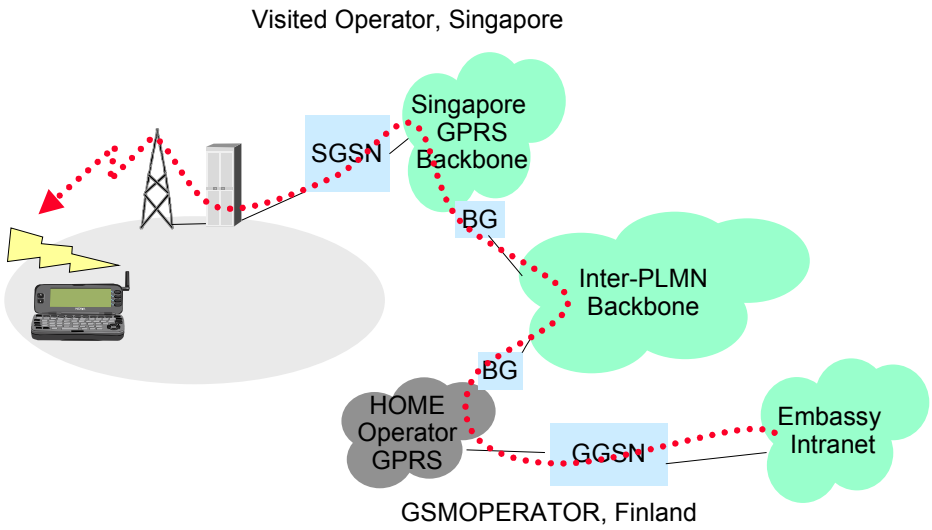

Figure 13. GPRS data transfer from the embassy server to the MS

The PDP context is active and the SGSN sends a notification to the MS. The diplomat can now download her e-mail from the embassy e-mail server in the embassy intranet. The packet transfer path is shown in Figure 13.

In the example we were using an access point in the home network. This is not the only option. A subscriber attached to the visited network could also use an access point provided by the visited network. The types of access points allowed are a part of the subscription data in HLR. HLR subscriber information includes flags that specify the following:

- User is allowed to use visited network access point
- User can select home or visited access point, or
- User needs to use the access points in the home network.

The connection between two operators' GPRS networks can be through one of two options as shown in :

a. Public data network (PDN) network, such as the Internet, in which a secure tunnel with encryption is set up between two GGSNs.

b. Private inter-PLMN network, which has the benefit of good control over quality and security.

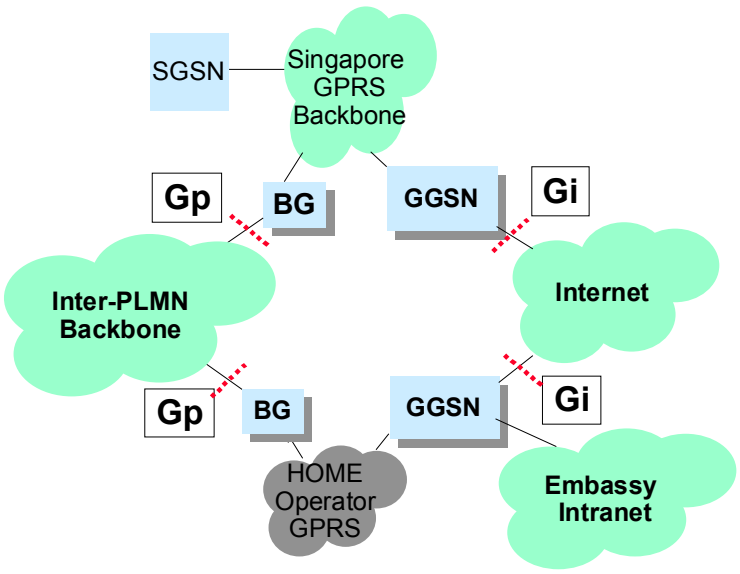

Figure 14. Connecting the GPRS networks of two PLMNs

6 Key points

- A GPRS network is expected to perform the functions of GSM network and data network.
- The new elements of the GPRS network are the PCU, SGSN, GGSN, CG, BG, DNS, and Firewalls.

- The functions of the Gateway GPRS Support Node (GGSN)are the following:
  - Routing mobile-destined packets from external networks to relevant SGSN
  - Routing packets originating from an MS to the correct external network
  - Interfacing to external IP networks
  - Collecting charging data and traffic statistics
  - Allocating dynamic IP addresses to mobiles either by itself or with the help of a DHCP or a RADIUS server.

- The functions of the Serving GPRS Support Node (SGSN) are the following:
  - Converting protocols used in IP backbone to protocols used in the BSS and MS
  - Handling of authentication and mobility management
  - Routing data to relevant GGSN when connecting to an external network
  - Collecting charging data and traffic statistics
  - Handling of ciphering and data compression.

- The interfaces in the GPRS network are the following:
  - **Gb** SGSN to BSS
  - **Gn** between GSNs (GTP)
  - **Gr** between SGSN and HLR (MAP)

© Nokia Networks Oy

- **Gs** SGSN to MSC (BSSAP+)
- **Gi** GGSN to external data networks
- **Gf** SGSN and the EIR (MAP)
- **Gd** between SGSN and the GMSC (SMSC)
- **Ga** between GSNs and CG.

- Tunnelling is the process by which user packets are transported encapsulated in containers and transported through a network.
- The tunnelling protocol in GPRS is called the GPRS Tunnelling Protocol (GTP) over the GPRS backbone. The backbone is an IP network.
- Tunnelling is used when:
  c. the packets with private IP addresses have to transmitted through a public network
  d. packets of one protocols have to be sent through a network that does not understand it
  e. for security reasons.

Appendix – GPRS transmission plane protocols

1. Overview of protocols used in GPRS

A GPRS network introduces many new protocols designed to convey user data in a reliable and secure way. Information is passed between the existing GSM network and the GPRS network by employing protocols on two separate planes:

- **Transmission plane protocols** are used for the transmission of user data and control functions.
- **Signalling plane protocols** are used to convey signalling information that controls and supports the transmission plane functions.

The transmission plane protocols convey user data in the form of IP datagrams from the mobile station to external networks, such as the Internet or corporate data networks.

The signalling plane contains many protocols that are already employed in existing GSM network elements.

1.1 GPRS transmission plane protocols

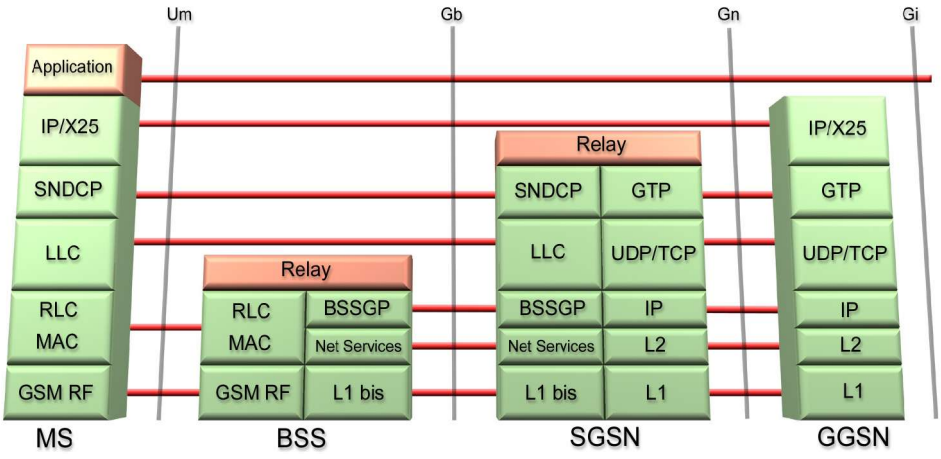

Figure 1. Transmission plane protocols

1.2 Transmission protocols in the Um interface

1.2.1 Physical layer

The physical layer can be divided into the **Radio Frequency (RF)** layer and the **Physical Link** layer.

The **Radio Frequency (RF)** is the normal GSM physical radio layer. Among other things the RF layer specifies:

- the carrier frequency characteristics and GSM radio channel structures
- the radio modulation scheme used for the data
- the radio transmitter and receiver characteristics as well as performance requirements.

The GSM RF physical layer is used for GPRS with the possibility for future modifications.

The **Physical Link** layer supports multiple MSs sharing a single physical channel and provides communication between the MSs and the network.

Network controlled handovers are not used in the GPRS service. Instead, routing area updates and cell updates are used.

The Physical Link layer is responsible for:

- Forward Error Correction (FEC) coding, allowing the detection and correction of transmitted code words and the indication of incorrectable code words
- the interleaving of one RLC Radio Block over four bursts in consecutive TDMA frames.

1.2.2 Medium Access Control (MAC)

The Medium Access Control (MAC) protocol handles the channel allocation and the multiplexing, that is, the use of physical layer functions. The RLC and the MAC together form the OSI Layer 2 protocol for the Um interface.

The GPRS MAC function is responsible for:

- Providing efficient multiplexing of data and control signalling on both the uplink and downlink. This process is controlled by the network. On the downlink, multiplexing is controlled by a scheduling mechanism. On

the uplink, multiplexing is controlled by medium allocation to individual users (for example, in response to a service request).

- Mobile originated channel access, contention resolution between channel access attempts, including collision detection and recovery.
- Mobile terminated channel access, scheduling of access attempts, including queuing of packet accesses.
- Priority handling.

1.2.3 The Radio Link Control (RLC)

The Radio Link Control (RLC) protocol offers a reliable radio link to the upper layers. Two modes of operation of the RLC layer are defined for information transfer: unacknowledged and acknowledged. The RLC layer can support both modes simultaneously.

The RLC function is responsible for:

- Providing transfer of Logical Link Control layer PDUs (LLC-PDU) between the LLC layer and the MAC function.
- Segmentation and reassembly of LLC-PDUs into RLC Data Blocks. See Figure 2.
- Backward Error Correction (BEC) procedures enabling the selective retransmission of uncorrectable code words. This process is generally known as Automatic Request for Retransmission (ARQ).

Note

The Block Check Sequence for error detection is provided by the Physical Link layer.

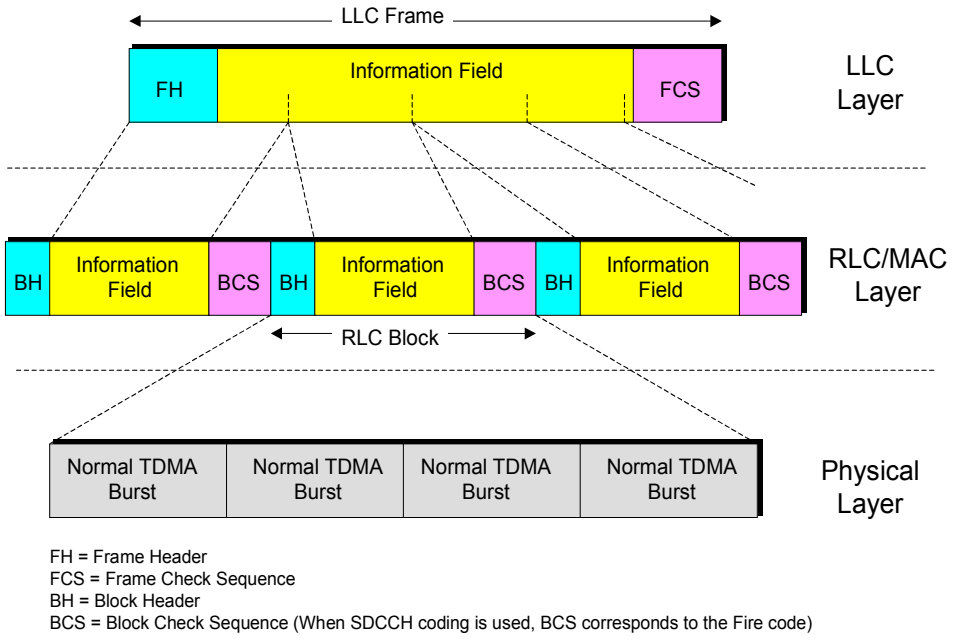

Figure 2. Segmentation of LLC-PDUs into RLC data blocks

1.2.4 Logical Link Control (LLC)

The Logical Link Control (LLC) layer offers a secure and reliable logical link between the MS and the SGSN for upper layer protocols, and is independent of the lower layers.

The LLC conveys signalling, SMS, and Subnetwork Dependent Convergence Protocol (SNDCP) packets. SNDCP exists between the MS and the SGSN and provides a mapping and compression function between the network layer (IP or X.25 packets) and the lower layers. It also performs segmentation, reassembly, and multiplexing.

Two modes of operation of the LLC layer are defined for information transfer: **unacknowledged and acknowledged**. The LLC layer can support both modes simultaneously.

In **acknowledged mode**, the receipt of LLC-PDUs is confirmed. The LLC layer retransmits LLC-PDUs if confirmation has not been received within a certain timeout period.

In **unacknowledged mode**, there is no confirmation required for LLU-PDUs.

Signalling and SMS is transferred in unacknowledged mode.

In unacknowledged mode, the LLC layer offers he following two options:

- Transport of **"protected"** information means that if errors occur within the LLC information field, the frame will be discarded.
- Transport of **"unprotected"** information means that if errors occur within the LLC information field, the frame will not be discarded.

The LLC layer supports several different QoS delay classes with different transfer delay characteristics.

The **Packet Control Unit (PCU) in the BSC** is responsible for the following GPRS MAC and RLC layer functions:

- LLC layer PDU segmentation into RLC blocks for downlink transmission.
- LLC layer PDU reassembly from RLC blocks for uplink transmission.
- PDCH scheduling functions for the uplink and downlink data transfers.
- PDCH uplink ARQ functions, including RLC block ack/nak.
- PDCH downlink ARQ function, including buffering and retransmission of RLC blocks.
- Channel access control functions, for example access requests and grants.
- Radio channel management functions, for example power control, congestion control, broadcast control information, etc.

The **Channel Coding Unit (CCU) in the BTS** provides the following functions:

- The channel coding functions (CS-1 and CS-2), including FEC and interleaving.
- Radio channel measurement functions, including received quality level, received signal level, and information related to timing advance measurements.

The network layer protocols for signalling, SMS, and user data are multiplexed to the lower layers in the following way (see Figure 3):

- **NSAPI** is the Network layer Service Access Point Identifier, which is used to identify the PDP context at the SNDCP level.
- **SAPI** is the Service Access Point Identifier, which is used to identify the points where the LLC provides a service to a higher layer. SAPIs have different priorities.
- **TLLI** is the Temporary Logical Link Identity, which unambiguously identifies the logical link between the MS and SGSN. TLLI is used for addressing at the LLC layer.

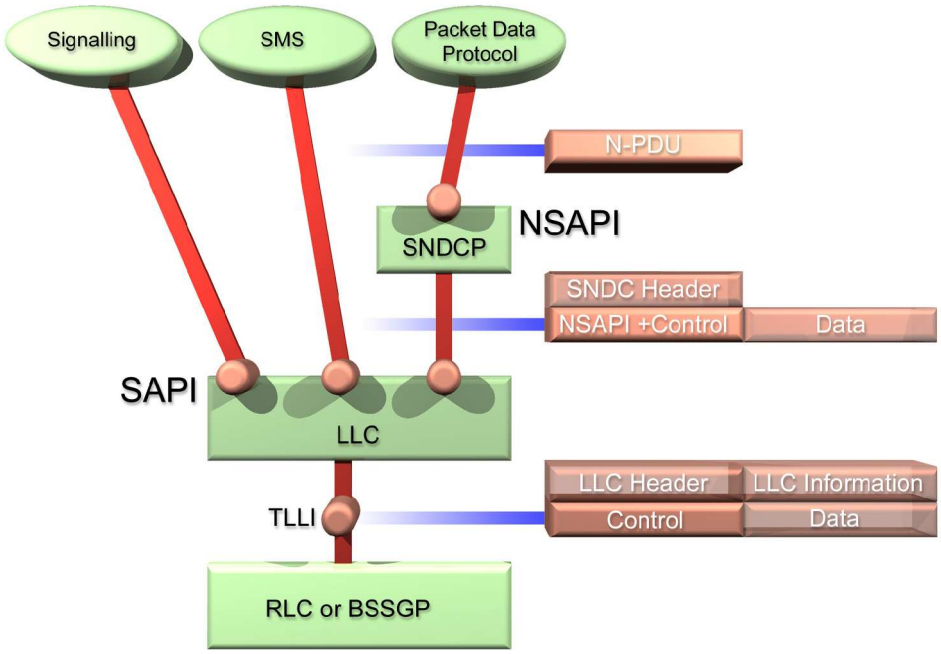

Figure 3. Multiplexing of network protocols

LLC provides the services necessary to maintain a ciphered data link between an MS and an SGSN. The LLC layer does not support direct communication between two MSs.

The LLC connection is maintained as the MS moves between cells served by the same SGSN. When the MS moves to a cell being served by a different SGSN, the existing connection is released and a new logical connection is established with the new SGSN.

LLC is independent of the underlying radio interface protocols. In order to allow LLC to operate with a variety of different radio interface protocols, and to ensure optimum performance, it may be necessary to adjust, for example, the maximum LLC PDU length and the LLC protocol timer values. Such adjustments can be made through negotiation between the MS and the SGSN. The maximum length of an LLC PDU shall not be greater than 1600 octets minus the BSSGP protocol control information.

The Logical Link Control layer supports:

- Service primitives allowing the transfer of SNDCP Protocol Data Units (SN-PDUs) between the Subnetwork Dependent Convergence layer and the Logical Link Control layer
- Procedures for transferring LL-PDUs between the MS and SGSN, including:
  - Procedures for unacknowledged point-to-point delivery of LL-PDUs between the MS and the SGSN
  - Procedures for acknowledged, reliable point-to-point delivery of LL-PDUs between the MS and SGSN
  - Procedures for point-to-multipoint delivery of LL-PDUs from the SGSN to the MS
- Procedures for detecting and recovering from lost or corrupted LL-PDUs
- Procedures for flow control of LL-PDUs between the MS and the SGSN
- Procedures for ciphering of LL-PDUs. The procedures are applicable to both unacknowledged and acknowledged LL-PDU delivery.

The Logical Link Control layer functions are organised so that ciphering resides immediately above the RLC/MAC layer in the MS, and immediately above the BSSGP layer in the SGSN.

A logical communication pipe is established between the GGSN and the MS through a SGSN. The LLC protocol link is established between the MS and the SGSN upon GPRS attach. The GPRS Tunnelling Protocol (GTP) establishes a tunnel between the SGSN and the GGSN at PDP context activation. In the LLC header, the NSAPI (Network layer Service Access Point Identifier) identifies which application inside the MS the packet belongs to.

© Nokia Networks Oy

1.2.5 SNDCP (Subnetwork Dependent Convergence Protocol)

Network layer protocols are intended to be capable of operating over a wide variety of subnetworks and data links. GPRS supports several network layer protocols providing protocol transparency for the users of the service.

To enable the introduction of new network layer protocols to be transferred over GPRS without any changes to GPRS, all functions related to the transfer of Network layer Protocol Data Units (N-PDUs) are carried out in a transparent way by the GPRS network. This is one of the requirements of SNDCP.

Another requirement of the SNDCP is to provide functions that help to improve channel efficiency. This is achieved by means of compression techniques.

The set of protocol entities above the SNDCP consists of commonly used network protocols. They all use the same SNDCP entity, which then performs multiplexing of data coming from different sources to be transferred using the service provided by the LLC layer. The Network Service Access Point Identifier (NSAPI) is an index to the PDP context of the PDP that is using the services provided by the SNDCP (see Figure 4). One PDP may have several PDP contexts and NSAPIs.

Each active NSAPI uses the services provided by the Service Access Point Identifier (SAPI) in the LLC layer. More than one NSAPIs may be associated with the same SAPI.

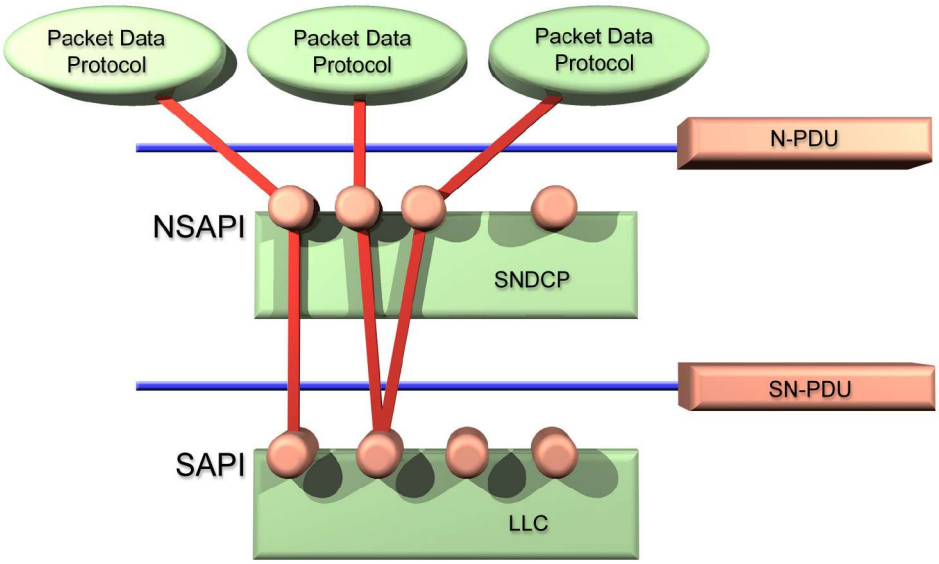

Figure 4. SNDCP used to multiplex different protocols

1.3 Transmission protocols in the Gb interface

The Gb interface allows many users to be multiplexed over the same physical link using Frame Relay (FR). Bandwidth is allocated to a user upon activity (when data is sent or received) and is reallocated immediately thereafter. This is, in contrast to the A-interface, where a single user has the exclusive use of a dedicated physical resource throughout the lifetime of a call irrespective of activity.

GPRS signalling and user data are sent in the same transmission plane and therefore no separate dedicated physical resources are required to be allocated for signalling purposes.

Data rates over the Frame Relay Gb interface may vary for each user without restriction, from zero data to the maximum possible line rate (for example 1984 kbit/s, which is the maximum available bit rate of a 2 Mbit/s (E1) link).

© Nokia Networks Oy

1.3.1 Physical Layer Protocol

Several physical layer configurations and protocols are possible at the Gb interface and the physical resources are allocated by Operation & Maintenance (O&M) procedures. Normally a G703/704 2Mbit/s connection is provided.

1.3.2 Network Services layer

The Gb interface Network Services layer is based on **Frame Relay**. Frame Relay virtual circuits are established between the SGSN and BSS. LLC PDUs from many users are statistically multiplexed onto these virtual circuits. These virtual circuits may traverse a network of Frame Relay switching nodes, or may just be provided on a point to point link between the BSC and the SGSN (if the BSC and SGSN are co-located). Frame Relay is used for signalling and data transmission over the Gb interface.

The following characteristics apply for the Frame Relay connection:

- The maximum Frame Relay information field size is 1600 octets.
- The Frame Relay address length is two octets.
- Frame Relay Permanent Virtual Circuits (PVC) are used.
- The Frame Relay layer offers detection of errors, but no recovery from errors.
- One or more Frame Relay PVCs are used between an SGSN and a BSS to transport BSSGP PDUs.

1.3.3 Base Station System GPRS Protocol (BSSGP)

The **Base Station System GPRS Protocol (BSSGP)** transfers control and signalling information and user data between a BSS and the SGSN over the Gb interface.

The primary function of BSSGP is to provide Quality of Service (QoS), and routing information that is required to transmit user data between a BSS and an SGSN.

A secondary function is to enable two physically distinct nodes, the SGSN and BSS, to operate node management control functions.

There is a one-to-one relationship between the BSSGP protocol in the SGSN and in the BSS. If one SGSN handles multiple BSSs, the SGSN has to have one BSSGP protocol device for each BSS.

The main functions for the BSSGP protocol are to:

- provide a connectionless link between the SGSN and the BSS
- transfer data in an unconfirmed way between the SGSN and the BSS
- provide for bi-directional control of the data flow between the SGSN and the BSS
- handle paging requests from the SGSN to the BSS
- give support for deleting old messages in the BSS, for example when an MS changes BSSs
- support multiple layer 2 links between the SGSN and the BSS.

1.4 Transmission protocols in the Gn interface

The Gn interface forms the GPRS backbone network.

1.4.1 Layer 1 and layer 2

The **L1** and the **L2 protocols** are vendor dependent OSI layer 1 and 2 protocols that carry the IP datagrams for the GPRS backbone network between the SGSN and the GGSN.

1.4.2 Internet Protocol (IP)

The **Internet Protocol (IP)** datagram in the Gn interface is **only used in the GPRS backbone network**. The GPRS backbone (core) network and the GPRS subscribers use different IP addresses. This makes the GPRS backbone IP network invisible to the subscribers and vice versa. The GPRS backbone network carries the subscriber IP or X.25 traffic in a secure GPRS tunnel.

All data from the mobile subscribers or external networks is tunnelled in the GPRS backbone.

1.4.3 TCP or UDP

TCP or UDP are used to carry the GPRS Tunnelling Protocol (GTP) PDUs across the GPRS backbone network. TCP is used for user X.25 data and UDP is used for user IP data and signalling in the Gn interface.

1.4.4 GPRS Tunnelling Protocol (GTP)

The **GPRS Tunnelling Protocol (GTP)** allows multi-protocol packets to be tunnelled through the GPRS backbone between GPRS Support Nodes (GSNs). This is illustrated in Figure 5.

The GTP can have proprietary extensions to allow proprietary features. The relay function in the SGSN relays the user PDP (Packet Data Protocol) PDUs (IP or X.25) between the Gb and the Gn interfaces.

GTP is defined both for the Gn interface, that is, the interface between GSNs within the same PLMN, and the Gp interface between GSNs in different PLMNs.

The UDP/IP and TCP/IP are examples of paths that may be used to multiplex GTP tunnels. The choice of path is dependent on whether the user data to be tunnelled requires a reliable link or not. Two modes of operation of the GTP layer are therefore supported for information transfer between the GGSN and SGSN.

- unacknowledged (UDP/IP)
- acknowledged (TCP/IP).

A UDP/IP path is used when the user data is based on connectionless protocols, such as IP. A TCP/IP path is used when the user data is based on connection-oriented protocols, such as X.25.

The GTP layer can support both modes simultaneously.

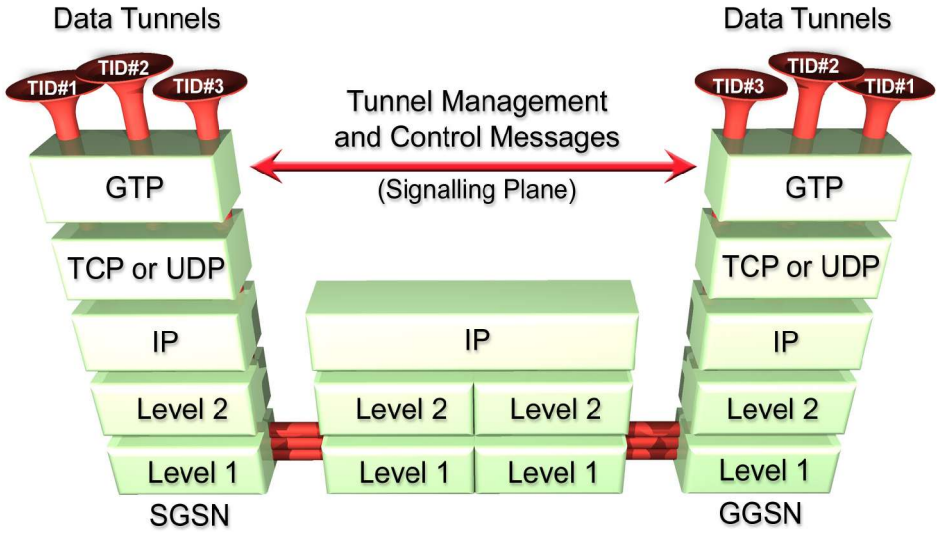

Figure 5. GPRS Tunnelling Protocol principle

1.4.4.1 Signalling plane

In the signalling plane, the GTP specifies a tunnel control and management protocol which allows the SGSN to provide GPRS network access for an MS. The signalling plane also handles path management and location management. Signalling is used to create, modify and delete tunnels.

The GTP signalling flow is logically associated with, but separate from, the GTP tunnels. For each GSN-GSN pair, one or more paths exist and one or more tunnels may use each path.

1.4.4.2 Transmission plane

In the transmission plane, the tunnel created by the signalling plane is used to carry user data packets between network elements connected to the GPRS backbone network, such as the SGSNs and GGSNs. No other systems need to be aware of GTP, for example, the MSs are connected to a SGSN without being aware of GTP.

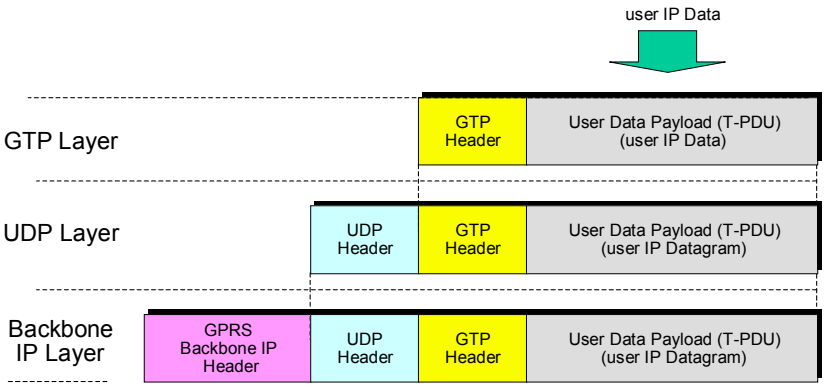

Figure 7. The GTP protocol header being added to user data

A GTP tunnel is defined by two associated PDP contexts in different GSN nodes and is identified by a Tunnel ID (TID). A GTP tunnel is necessary for forwarding packets between an external packet data network and an MS. The Tunnel ID identifies the MM and PDP contexts (MM Context ID and a NSAPI).

The NSAPI (Network Service Access Point Identifier) is a fixed value between 0 and 15 that identifies a certain PDP context. It identifies a PDP context belonging to a specific MM context ID.

1.4.5 The GTP header

The GTP header contains 16 octets and is used for all GTP messages.

The information contained in the GTP header includes the following:

- The type of GTP message (signalling messages = 1-52, but when used for data transmission the GTP message type = 255).
- The length of the GTP message (G-PDU) in octets.
- A Sequence Number to provide a transaction identity for signalling messages and a growing sequence number for tunnelled T-PDUs. (A T-PDU is an IP datagram from an MS or a network node in an external packet data network. The T-PDU is the payload that is tunnelled in the GTP tunnel).
- A flag to indicate whether an LLC frame number is included or not.

- An LLC frame number that is used for the Inter SGSN Routing Update procedure to co-ordinate the data transmission on the link layer between the MS and the SGSN.
- A TID (Tunnel Identifier) that points out MM and PDP contexts.

The content of the GTP header differs depending on whether the header is used for signalling messages or user data (T-PDUs).

1.4.6 Tunnel ID (TID) format

The Tunnel Identifier (TID) consists of the following:

- Mobile Country Code (MCC)
- Mobile Network Code (MNC)
- Mobile Subscriber Identification Number (MSIN)
- Network Service Access Point Identifier (NSAPI)

These represent the MM and PDP contexts.

© Nokia
Networks Oy

References

Nokia DX200 SGSN Product Description

Nokia GPRS Charging Gateway Product Description

Nokia GN2500 GGSN Product Description

Nokia GPRS Solution Description

Nokia GPRS System Description

GSM Specification 03.60 (GPRS Service Description R.97)

GSM Specification 03.64 (Overall Desc. GPRS Radio Interf. R.97)

GSM Specification 04.08

GSM Specification 04.11

GSM Specification 04.64

GSM Specification 04.65

GSM Specification 07.60

GSM Specification 07.70

GSM Specification 08.14

GSM Specification 08.16

GSM Specification 08.18

GSM Specification 09.02

GSM Specification 09.16

GSM Specification 09.18

GSM Specification 09.60

GSM Specification 12.15

Abbreviations

AoCC	Advice of Charge - Charging
AoCI	Advice of Charge - Information
AP	Access Point
ATM	Asynchronous Transfer Mode
AuC	Authentication Centre
BCCH	Broadcast Control Channel
BG	Border Gateway
BGIWP	Barring of GPRS Interworking Profile(s)
BGP	Border Gateway Protocol
BSC	Base Station Controller
BSS	Base Station Subsystem
BSSAP	BSS Application Part
BSSGP	BSS GPRS Protocol
BSSMAP	BSS Management Application Process
BTS	Base Transceiver Station
BTSM	BTS Management
CC	Call Control
CCBS	Customer Care and Billing System
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CDR	Call Detail Record
CFNRc	Call Forwarding on Mobile Subscriber Not Reachable
CFU	Call Forwarding Unconditional
CG	Charging Gateway
CG/AD	CG/Alarm Dispatcher
CG/ARC	CG/Accounting Record Collection
CG/ARM	CG/Accounting Record Modification
CG/FTM	CG/File Transfer Manager

© Nokia Networks Oy

CLNS	Connectionless Network Service
CM	Communication Management
CONS	Connection-Oriented Network Service
CUG	Closed User Group
DAMPS	Digital Advanced Mobile Phone Service
DB	Database
DCS	Digital Cellular System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRX	Discontinuous Reception
DTAP	Direct Transfer Application Process
EDGE	Enhanced Data Rates for GSM Evolution
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
ETSI	European Telecommunications Standards Institute
FDMA	Frequency Division Multiple Access
FTAM	File Transfer, Access and Management
FTMID	Sequential number of method instance
FTP	File Transfer Protocol
G-CDR	Gateway GPRS Support Node-Call Detail Record
GGSN	Gateway GPRS Support Node
GMSC	Gateway MSC
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GSN	GPRS Support Node
GTP	GPRS Tunnelling Protocol
GTP´	GPRS Tunnel Protocol (enhanced)
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
HSCSD	High Speed Circuit Switched Data

HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IGRP	Interior Gateway Routing Protocol
IMEI	International Mobile Equipment Identity
IMGI	International Mobile Group Identity
IMSI	International Mobile Subscriber Identity
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
ITU-T	Telecommunication standardisation sector of ITU
LA	Location Area
LAN	Local Area Network
LAPD	Link Access Protocol for the D channel
LAPDm	Link Access Protocol for the Dm channel
LLC	Logical Link Control
MAC	Medium Access Control
MAP	Mobile Application Part
M-CDR	Mobility Management-Call Detail Record
ME	Mobile Equipment
MIB-II	Management Information Base II
MM	Mobility Management
MoU	Memorandum of Understanding
MS	Mobile Station
MSC	Mobile (services) Switching Centre
MT	Mobile Termination

© Nokia Networks Oy

MTP	Message Transfer Part
NFS	Network File System
NMS	Network Management Subsystem
NSAPI	Network layer Service Access Point Identifier
NSS	Network and Switching Subsystem
OMC	Operations and Maintenance Centre
OSI	Open System Interconnection
OSPF	Open Shortest Path First
OSS	Operation Subsystem
PACCH	Packet Associated Control Channel
PAD	Packet Assembly/Disassembly